P10310?

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－259223
（Ｐ2002－259223Ａ）
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード*(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｆ	５Ｂ０１７
15/00	３３０	15/00	３３０Ｚ	５Ｂ０８５
17/60	ＺＥＣ	17/60	ＺＥＣ	５Ｃ０６４
	１４２		１４２	５Ｊ１０４
	３０２		３０２Ｅ	

審査請求　有　請求項の数18　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願2001－53193(Ｐ2001－53193)

(22)出願日　平成13年２月27日(2001.2.27)

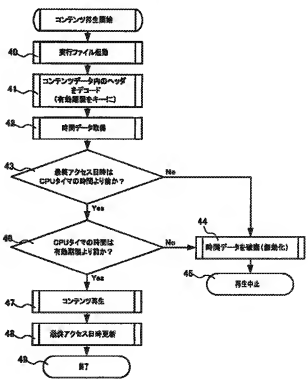
(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　ニュー　オーチャード　ロード

(74)復代理人　100112520
弁理士　林　茂則　（外２名）

最終頁に続く

(54)【発明の名称】　コンテンツ利用方法、コンテンツ配信方法、コンテンツ配信システムおよびプログラム

(57)【要約】
【課題】　コンテンツ利用に有効期限を設けた場合に、ユーザの不正なコンテンツ利用を防止する。
【解決手段】　コンテンツまたはコンテンツ実行プログラムに有効期限を示す情報を持たせる。有効期限情報は、たとえば外部ファイル、コンテンツまたはコンテンツ実行プログラムに埋め込む。また、有効期限情報は、利用開始日時、利用終了日時、最終利用日時とする。これらデータを認証データとして、コンテンツの利用時（コンテンツ実行プログラムの実行時）に認証を行う。認証の手法として、たとえば、コンテンツ利用の際に、（１）システムタイマから取得される現在日時が利用開始日時と利用終了日時（有効期限）の間にあること、（２）現在日時が最終利用日時（最終アクセス日時）よりあとであること、の２つの要件を満足する場合にのみ実行プログラムの実行を許可する。



1

【特許請求の範囲】

【請求項１】　コンテンツの利用開始日時を特定する利用開始日時と、コンテンツ利用の有効期限を特定する利用終了日時と、コンテンツが最後に利用された日時を特定する最終利用日時とを含む認証データを取得するステップと、

コンテンツの利用に際して、現在日時をシステムタイマから取得するステップと、

前記最終利用日時が前記現在日時より前であるかを判断する第１判断ステップと、

前記現在日時が、前記利用終了日時より前であるかを判断する第２判断ステップと、

前記第１および第２判断ステップの何れのステップにおいても、その判断が真の場合に前記コンテンツを再生または実行するステップと、

前記コンテンツの再生または実行の終了により、その終了日時で前記最終利用日時を更新するステップと、

をする方法。

【請求項２】　前記コンテンツの全体または一部が、前記認証データに含まれる暗号化データで符号化されており、

符号化されたコンテンツを前記暗号化データで復号化するステップをさらに有する請求項１記載のコンテンツの利用方法。

【請求項３】　前記第１判断ステップまたは第２判断ステップの何れかのステップにおいて、その判断が偽の場合、前記暗号化データを破棄するステップをさらに有する請求項２記載のコンテンツの利用方法。

【請求項４】　前記認証データは、隠しファイルとして生成されたファイル内に格納される第１の方法、または、前記コンテンツに埋め込まれる第２の方法、または、前記コンテンツを再生または実行するプログラムに埋め込まれる第３の方法、の何れかの方法で記録される請求項１記載のコンテンツの利用方法。

【請求項５】　コンテンツのダウンロード要求に応答して、前記要求を受け付けた時刻を用いてコンテンツの利用開始日時を特定する利用開始日時と、コンテンツ利用の有効期限を特定する利用終了日時とを含む認証データを生成するステップと、

前記コンテンツ、前記コンテンツの再生または実行プログラムおよび前記認証データ、または、これらを符号化したファイルを送信するステップと、を有し、

前記再生または実行プログラムは、その処理実行に際して、

現在日時をシステムタイマから取得する機能と、

前記コンテンツの最終利用日時が前記現在日時より前であるかを判断する第１判断機能と、

前記現在日時が、前記利用終了日時より前であるかを判断する第２判断機能と、

前記第１および第２判断の何れの判断においてもその判

2

断が真の場合に前記コンテンツを再生または実行する機能と、

前記コンテンツの再生または実行の終了により、その終了日時で前記最終利用日時を更新する機能と、をコンピュータに実現させるものである、

コンテンツ配信方法。

【請求項６】　前記コンテンツの全部または一部を前記認証データに含まれる暗号化データで符号化するステップをさらに有し、

前記再生または実行プログラムは、前記符号化されたコンテンツを前記暗号化データを用いて復号化する機能をさらに有するものである請求項５記載のコンテンツ配信方法。

【請求項７】　前記再生または実行プログラムは、前記第１判断機能または第２判断機能において、その判断が偽の場合、前記暗号化データを破棄する機能をさらに有するものである請求項６記載のコンテンツ配信方法。

【請求項８】　前記認証データは、前記再生または実行プログラムが実行されるシステムの隠しファイルとして生成されたファイル内に格納される第１の方法、または、前記コンテンツに埋め込まれる第２の方法、または、前記再生または実行するプログラムに埋め込まれる第３の方法、の何れかの方法で記録される請求項５記載のコンテンツ配信方法。

【請求項９】　コンテンツのダウンロード要求に応答して、前記要求を受け付けた時刻を用いてコンテンツの利用開始日時を特定する利用開始日時と、コンテンツ利用の有効期限を特定する利用終了日時とを含む認証データを生成する手段と、

前記コンテンツ、前記コンテンツの再生または実行プログラムおよび前記認証データ、または、これらを符号化したファイルを送信する手段と、を有し、

前記再生または実行プログラムは、その処理実行に際して、

現在日時をシステムタイマから取得する機能と、

前記コンテンツの最終利用日時が前記現在日時より前であるかを判断する第１判断機能と、

前記現在日時が、前記利用終了日時より前であるかを判断する第２判断機能と、

前記第１および第２判断の何れの判断においてもその判断が真の場合に前記コンテンツを再生または実行する機能と、

前記コンテンツの再生または実行の終了により、その終了日時で前記最終利用日時を更新する機能と、をコンピュータに実現させるものである、

コンテンツ配信システム。

【請求項１０】　前記コンテンツの全部または一部を前記認証データに含まれる暗号化データで符号化する手段をさらに有し、

前記再生または実行プログラムは、前記符号化されたコ

ンテンツを前記暗号化データを用いて復号化する機能をさらに有するものである請求項９記載のコンテンツ配信システム。

【請求項１１】　前記再生または実行プログラムは、前記第１判断機能または第２判断機能において、その判断が偽の場合、前記暗号化データを破棄する機能をさらに有するものである請求項１０記載のコンテンツ配信システム。

【請求項１２】　前記認証データは、前記再生または実行プログラムが実行されるシステムの隠しファイルとして生成されたファイル内に格納される第１の手段、または、前記コンテンツに埋め込まれる第２の手段、または、前記再生または実行するプログラムに埋め込まれる第３の手段、の何れかの手段で記録される請求項９記載のコンテンツ配信システム。

【請求項１３】　コンテンツの利用開始日時を特定する利用開始日時と、コンテンツ利用の有効期限を特定する利用終了日時と、コンテンツが最後に利用された日時を特定する最終利用日時とを含む認証データを取得する機能と、

現在日時をシステムタイマから取得する機能と、

前記最終利用日時が前記現在日時より前であるかを判断する第１判断機能と、

前記現在日時が、前記利用終了日時より前であるかを判断する第２判断機能と、

前記第１および第２判断機能の何れの判断においてもその判断が真の場合に前記コンテンツを再生または実行する機能と、

前記コンテンツの再生または実行の終了により、その終了日時で前記最終利用日時を更新する機能と、

をコンピュータに実現させるコンテンツを利用するためのプログラム。

【請求項１４】　前記コンテンツの全体または一部が、前記認証データに含まれる暗号化データで符号化されており、

前記プログラム製品が、

符号化されたコンテンツを前記暗号化データで復号化する機能と、

前記第１判断機能または第２判断機能の何れかの判断において、その判断が偽の場合、前記暗号化データを破棄する機能と、をさらに有する請求項１３記載のプログラム。

【請求項１５】　前記コンテンツを利用するコンピュータシステムに、そのシステムの稼動中または前記システム上で稼動するＯＳの稼動中に常時稼動しているカウンタ機能を実現するプログラムを有し、

前記システムの稼動開始または前記ＯＳの稼動開始の際に、前記プログラムで実現されたカウンタの時刻をシステムタイマから取得した日時で初期化するステップと、

前記コンテンツの利用の際に、前記カウンタによる日時とシステムタイマから取得した日時との差分を記録するステップと、

前記差分に相当する期間で、前記最終利用日時および前記利用終了日時、または、前記現在日時を補正するステップと、

をさらに含む請求項１記載のコンテンツ利用方法。

【請求項１６】　前記コンテンツ、前記コンテンツの再生または実行プログラムおよび前記認証データ、または、これらを符号化したファイルを送信するステップにおいて、システムの稼動中または前記システム上で稼動するＯＳの稼動中に常時稼動しているカウンタ機能を実現するプログラムを同時に送付し、

前記カウンタ機能を実現するプログラムは、前記システムの稼動開始または前記ＯＳの稼動開始の際に、前記カウンタ機能による時刻をシステムタイマから取得した日時で初期化する機能と、前記システムタイマとは独立に時刻をカウントする機能とをコンピュータに実現させるものであり、

前記再生または実行プログラムは、その処理に際して、前記カウンタ機能による日時とシステムタイマから取得した日時との差分を記録する機能と、前記差分に相当する期間で、前記最終利用日時および前記利用終了日時、または、前記現在日時を補正する機能と、をさらにコンピュータに実現させるものである請求項５記載のコンテンツ配信方法。

【請求項１７】　前記コンテンツ、前記コンテンツの再生または実行プログラムおよび前記認証データ、または、これらを符号化したファイルを送信する手段において、システムの稼動中または前記システム上で稼動するＯＳの稼動中に常時稼動しているカウンタ機能を実現するプログラムを同時に送付し、

前記カウンタ機能を実現するプログラムは、前記システムの稼動開始または前記ＯＳの稼動開始の際に、前記カウンタ機能による時刻をシステムタイマから取得した日時で初期化する機能と、前記システムタイマとは独立に時刻をカウントする機能とをコンピュータに実現させるものであり、

前記再生または実行プログラムは、その処理に際して、前記カウンタ機能による日時とシステムタイマから取得した日時との差分を記録する機能と、前記差分に相当する期間で、前記最終利用日時および前記利用終了日時、または、前記現在日時を補正する機能と、をさらにコンピュータに実現させるものである請求項９記載のコンテンツ配信システム。

【請求項１８】　システムの稼動開始または前記ＯＳの稼動開始の際に、前記カウンタ機能による時刻をシステムタイマから取得した日時で初期化する機能と、前記システムタイマとは独立に時刻をカウントする機能とをコンピュータに実現させるカウンタプログラムから日時を取得する機能と、

前記カウンタプログラムによる日時とシステムタイマから取得した日時との差分を記録する機能と、
前記差分に相当する期間で、前記最終利用日時および前記利用終了日時、または、前記現在日時を補正する機能と、
をさらにコンピュータに実現させる請求項１３記載のプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンテンツの配信方法、システムおよびそれらを実現するソフトウェアに関し、特に、コンテンツの利用に有効期限を設ける場合に適用して有効な技術に関する。

【０００２】

【従来の技術】インターネット等、ネットワーク技術の進展により、画像、映像、音声、アプリケーションソフトウェア等のディジタルコンテンツのネットワーク配信が商業ベースで行われるようになっている。これらディジタルコンテンツのネットワーク配信は、ＣＤ－ＲＯＭ等の媒体にコンテンツを記録して販売される場合のように、媒体の製造、在庫、流通、店頭による販売等が必要でなく、ディジタルコンテンツ（情報）の販売を拡大する有望な手法として期待される。すなわちネットワーク配信では情報をやり取りするだけでユーザにコンテンツを渡すことができ、適当な決済手段を併用することにより、ほぼ自動的にコンテンツの直接販売を完了できる。販売者側は人員、設備、資産等の経営資源を削減でき、一方ユーザにとっては任意の場所で好きな時間に迅速にコンテンツを入手することができる。コンテンツのネットワーク配信は、両者にとってその利便性が極めて高く、販売コストの削減、ひいては販売価格の低減を図ることが可能になる。

【０００３】しかしながらディジタルコンテンツはディジタル情報であるため本質的に複製が可能であり、複製による品質の劣化が極めて少ない。また、複製されたコンテンツは、ネットワークを用いればほぼ瞬時に世界的な規模で流布することが可能であり、コンテンツ所有者の著作権等の利益を大きく侵害することになる。このため、複製防止の技術が重要であり、一般に各種の認証手段をコンテンツの実行プログラムに備えて、認証を得たものだけが実行プログラムを起動してコンテンツを利用できるようにしている。

【０００４】一方、コンテンツの利用には有効期限が設けられる場合がある。たとえば特定目的のアプリケーションソフトウェアを試用期間として配布する場合や、廉価に配布されるシェアウェアの場合である。あるいは、課金目的に音楽ソフトや映画等の映像ソフトを配信する場合にも有効期限が設けられる場合がある。このように有効期限を設けてコンテンツを販売することにより、コンテンツの利用の機会を拡大し、あるいはコンテンツ利用の料金を安くして、コンテンツの利用促進を図ることが可能になる。

【０００５】コンテンツに有効期限を設けるには、たとえばコンテンツあるいはコンテンツ実行プログラムに有効期限情報を持たせ、プログラムを実行するコンピュータ等情報処理装置のシステムタイマを用いて期限が経過しているか否かを判断する手法が一般的である。なお、インターネットからの配信データに有効期限を付す技術として、たとえば特開平１１－３１１３０号公報に記載の技術がある。

【０００６】

【発明が解決しようとする課題】しかしながら、前記した従来技術のみでは、利用者の不正使用を簡単に許す場合がある。すなわち、前記複製防止手段によりコンテンツあるいはその実行プログラムの不正な複製は防止できる。ところが、複製防止手段だけではコンテンツの利用に有効期限を設けた場合の不正な使用を有効に防止できない。つまり、従来技術においては、コンテンツ利用の有効期限をその実行プログラムが走るコンピュータのシステムタイマを用いて判断するので、ユーザが故意にシステムタイマを変更してその日時を有効期限内に戻した場合には、実際には有効期限を渡過した場合であってもコンテンツの利用・再生が可能になる。これではコンテンツ利用に有効期限を設けた意義がなくなってしまう。

【０００７】本発明の目的は、コンテンツ利用に有効期限を設けた場合に、ユーザの不正なコンテンツ利用を防止する技術を提供することにある。

【０００８】

【課題を解決するための手段】本願の発明の概略を説明すれば、以下の通りである。すなわち、本発明は、コンテンツまたはコンテンツ実行プログラムに有効期限を示す情報を持たせる。有効期限情報は、たとえば外部ファイル、コンテンツまたはコンテンツ実行プログラムに埋め込むことができる。また、有効期限情報は、利用開始日時、利用終了日時（有効期限）、最終利用日時とすることができ、これらデータを認証データとして、コンテンツの利用時（コンテンツ実行プログラムの実行時）に認証を行うことができる。認証の手法として、たとえば、コンテンツ利用の際に、（１）システムタイマから取得される現在日時が利用開始日時と利用終了日時の間にあること（あるいは現在日時が利用終了日時前であること）、（２）現在日時が最終利用日時よりあとであること、の２つの要件を満足する場合にのみ実行プログラムの実行を許可することにより行う。

【０００９】このようなコンテンツの実行方法を用いることにより、有効期限内でのコンテンツの利用が許可されるとともに、仮にユーザが不正にシステムタイマを戻しても、前記（２）の要件を満たさない場合には、コンテンツの利用を制限することができ、有効期限が付されたコンテンツの不正な利用を防止できる。

【００１０】また、本発明では、システムタイマとは独立にそのシステムまたはＯＳの稼動中に独立した時刻をカウントするカウンタを設け、コンテンツ実行の際に、このカウンタから取得した時刻とシステムタイマの時刻とに差がある場合には、この差分に相当する期間で利用終了日時（有効期限）を補正することができる。これにより、最終利用日時と利用終了日時（有効期限）の間をターゲットにした時刻変更による不正使用の継続を防止できる。

【００１１】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。ただし、本発明は多くの異なる態様で実施することが可能であり、本実施の形態の記載内容に限定して解釈すべきではない。なお、実施の形態の全体を通して同じ要素には同じ番号を付するものとする。

【００１２】以下の実施の形態では、主に方法またはシステムについて説明するが、当業者であれば明らかなとおり、本発明はコンピュータで使用可能なプログラムとしても実施できる。したがって、本発明は、ハードウェアとしての実施形態、ソフトウェアとしての実施形態またはソフトウェアとハードウェアとの組合せの実施形態をとることができる。プログラムは、ハードディスク、ＣＤ－ＲＯＭ、光記憶装置または磁気記憶装置等の任意のコンピュータ可読媒体に記録できる。

【００１３】また以下の実施の形態では、一般的なコンピュータシステムを用いることができる。実施の形態で用いることができるコンピュータシステムは、中央演算処理装置（ＣＰＵ）、主記憶装置（メインメモリ：ＲＡＭ）、不揮発性記憶装置（ＲＯＭ）、コプロセッサ、画像アクセラレータ、キャッシュメモリ、入出力制御装置（Ｉ／Ｏ）等、一般的にコンピュータシステムに備えられるハードウェア資源を備える。また、ハードディスク装置等の外部記憶装置、インターネット等のネットワークに接続可能な通信手段を備えることができる。コンピュータシステムには、パーソナルコンピュータ、ワークステーション、メインフレームコンピュータ等各種のコンピュータが含まれる。

【００１４】図１は、本発明の一実施の形態であるコンテンツ配信方法を実現するシステムの一例を示した概念図である。本実施の形態のコンテンツ配信システムは、インターネット１に、コンテンツの配信を要求する端末、たとえばコンピュータシステム２、携帯電話３、携帯情報端末（ＰＤＡ：Personal Digital Assistants）４と、コンテンツを配信するサーバ５とが接続されている。コンテンツ配信先端末（コンピュータシステム２、携帯電話３、携帯情報端末４：以下単に端末という）は、サーバ５に対し、コンテンツ配信要求を発し、それに応えてサーバ５はコンテンツおよび認証データを端末に配信する。コンテンツおよび認証データを受信した端末は、後に詳しく説明するような手段を用いてコンテンツの再生あるいは実行を行い、ユーザの利用に供する。

【００１５】インターネット１は、良く知られているように、ＩＰ（Internet Protocol）に従って通信が行われる世界的に開かれたネットワークの一形態である。ここではインターネットを例示するが、他のネットワーク形態を利用することも可能である。たとえば専用電話線により接続されたネットワークあるいはＣＡＴＶ等のケーブルネットワークでもよい。インターネットの概念には、一般に利用が制限されるイントラネットも含む。また、ここではインターネット等の通信手段を介してサーバ５と端末とが接続される例を説明するが、ネットワークを介して前記要求および配信が行われる必要も無い。たとえば郵便、電話等によるユーザからの要求に応えて、サーバ５を管理する事業者が、たとえばＣＤ－ＲＯＭ等の媒体を介してコンテンツおよび認証データを配送してもよい。ただし、ネットワークを利用しない場合には、後述のダウンロードプログラムを利用できないので、後述の圧縮ファイルと認証データ２を配布することになる。

【００１６】コンピュータシステム２は、前記した一般的なコンピュータシステムであり、インターネット１に接続するための一般的な通信手段を有する。携帯電話３は、電話機能に加え、たとえば１モード等インターネット対応のデータ通信機能を備える。携帯情報端末４は、一部の機能が制限されるものの基本的にはコンピュータシステム同様の機能を備え、インターネットに接続するための通信機能を備える。コンピュータシステム２、携帯電話３、携帯情報端末４には、たとえばＨＴＴＰ（Hypertext Transfer Protocol）リクエストを発する適当なブラウザソフトがインストールされていることが好ましい。サーバ５は、前記した一般的なコンピュータシステムであり、適当な通信手段を備える。

【００１７】図２は、端末側のシステム（クライアント）とサーバ５のシステムを示したブロック図である。クライアント側のシステムには、たとえばブラウザ６、コンテンツ７、認証ファイル８、実行プログラム９、通信手段１０を有する。サーバ側のシステムには、たとえば時間情報生成手段１１、認証ファイル生成手段１２、ダウンロードプログラムファイル生成手段１３、圧縮ファイル生成手段１４、コンテンツ１５、通信手段１６を有する。なお、図２のクライアント側のシステムは、ダウンロードプログラムファイルが実行された後の状態を示す。

【００１８】クライアント側システムのブラウザ６は、インターネット１に接続し、サーバ５にＨＴＴＰリクエストを発するために用いる。一般的なブラウザが例示できる。

【００１９】コンテンツ７は、サーバ５からダウンロードされ、利用可能な状態にあるコンテンツデータであ

る。コンテンツには、たとえば音声ファイル、映像ファイル、アプリケーションプログラム等ユーザの利用対象のソフトウェア資源を例示できる。

【００２０】認証ファイル８は、後に詳しく説明するように、コンテンツのダウンロードに際に参照される認証１データ、コンテンツの解凍の際に参照される認証２データ、コンテンツの再生・実行の際に参照される認証３データを含む。これら認証データは隠しファイルとして保存することが好ましい。隠しファイルとすることにより、ユーザの改ざんを防止することができる。また、隠しファイルとすることに加えて、この認証ファイルのエディットデート（ファイル生成、変更日時）をＯＳのインストール日時に書き換えることも有効である。これによりユーザが隠しファイルを探索することを困難にし、その改ざんの防止をより有効にすることができる。

【００２１】実行プログラム９は、コンテンツ７を再生・実行するためのプログラムである。たとえばＭＰ３再生プログラム、ＭＰＥＧ再生プログラムや、アプリケーションプログラムを起動するためのプログラムが例示できる。

【００２２】通信手段１０は、サーバ５の通信手段１６と協働してインターネット１を介してデータを通信する。

【００２３】サーバ５の時間情報生成手段１１は、クライアントからダウンロード要求があったときに、その時点の日時と有効期間後の日時（有効期限）を生成し、主に前記認証３データに含まれる利用開始日時および利用終了日時に相当するデータを生成する。

【００２４】認証ファイル生成手段１２は、前記した時間情報生成手段１１により生成された時間情報から認証３データを生成し、また、前記認証１データおよび認証２データを自動的に生成する。認証１データは、圧縮されたコンテンツファイル（認証２データを含む）の格納先を示し、ダウンロードプログラムによって利用される。認証２データは、圧縮ファイルの解凍に用いられる。認証３データは、解凍されたコンテンツの利用（再生・実行）の際に用いられる。

【００２５】ダウンロードプログラムファイル生成手段１３は、後に説明する圧縮ファイルをダウンロードするためのプログラムファイルを生成する。ダウンロードプログラムファイルには、前記した認証１データが埋め込まれる。

【００２６】圧縮ファイル生成手段１４は、符号化された実行プログラム、認証３データおよびコンテンツを生成する。圧縮ファイルには前記した認証２データが埋め込まれる。実行プログラムおよびコンテンツの符号化は、認証２データを用いて復号化できるようにスクランブルをかける。スクランブルには、たとえばデータヒドゥン形式、ビットシフト形式を用いることができる。圧縮ファイルはクライアント側で実行した場合に自己解凍形式で解凍されることが好ましい。また、圧縮ファイルは前記認証１データで指定されるアドレスに格納される。

【００２７】コンテンツ１５は、ユーザによる利用対象のソフトウェア資源である。本実施の形態では、コンテンツ１５自体がユーザにダウンロードされるわけではない。

【００２８】図３は、本実施の形態のコンテンツ配信方法の一例を示したフローチャートである。まず、クライアント側からサーバ５にコンテンツの配信リクエストを行う（ステップ２０）。リクエストはたとえばＨＴＴＰリクエストである。

【００２９】このリクエストを受け付けたサーバ５は、時間情報を生成する（ステップ２１）。時間情報は、時間情報生成手段１１によってサーバ５のシステムタイマを用いて生成される。前記要求を受け付けた日時（利用開始日時）、および、利用開始日時に有効期間を加えた日時（利用終了日時すなわち有効期限）が生成される。

【００３０】次にサーバ５は、認証ファイル生成手段１２によって認証ファイルを生成する（ステップ２２）。認証ファイルには、前記のとおり認証１～３のデータがある。認証１データはサーバ内の任意のアドレスが指定され、認証２データはランダムに生成される。認証３データのうち利用開始日時、利用終了日時は前記時間情報生成手段によって生成された時間が適用される。認証３データのうち、最終利用日時（最終アクセス日時）は、未だ利用されていないので任意の値にできるが、ここでは利用開始日時とする。

【００３１】次にサーバ５は、前記認証１データを埋め込んだダウンロードプログラムファイルをダウンロードプログラムファイル生成手段１３により生成し、これをクライアントに送信する（ステップ２３）。

【００３２】さらに、サーバ５は、クライアントからの圧縮ファイル要求に備えて、圧縮ファイル生成手段１４により圧縮ファイルを生成する。生成された圧縮ファイルは認証１データで指定されたアドレスに格納する（ステップ２４）。

【００３３】一方、ダウンロードプログラムファイルを受信したクライアントは、ダウンロードプログラムを起動する（ステップ２５）。プログラムの起動は、受信完了により自動起動されても良い。

【００３４】次に、クライアントはダウンロードプログラムファイルに埋め込まれた認証１データを認証ファイル８に格納し（ステップ２６）、ダウンロードプログラムの処理にしたがって、圧縮ファイルのダウンロード要求を行う（ステップ２７）。このとき、ダウンロード要求は、認証１データで参照されるアドレスに格納されているファイルをダウンロードするように行い、よって、認証１データで参照されるアドレスにファイルが存在しない場合には圧縮ファイルのダウンロードは行われな

い。つまり、ダウンロードプログラムを仮にユーザがコピーして第三者に渡しても、第三者は認証１データが格納された隠しファイルを持たないため圧縮ファイルのダウンロードはできない。これにより不正コピーされたダウンロードプログラムファイルを無効化し、第三者による不正コピーを防止できる。

【００３５】圧縮ファイルの送信要求を受け付けたサーバ５は、認証１データで参照されるアドレスのファイルを送信する（ステップ２８）。このファイルは前記ステップ２４で処理されたとおりであれば、目的の圧縮ファイルであるはずである。

【００３６】圧縮ファイルを受信するクライアントでは、圧縮ファイルから認証２データを分離し、この認証２データを隠しファイルに格納する（ステップ２９）。圧縮ファイルの受信が完了すれば（ステップ３０）、これを受けてサーバ５では認証１データを無効化する。これにより再度のあるいは不正なダウンロードを防止できる。

【００３７】クライアントでは、圧縮ファイルのダウンロードの完了を受けて、その解凍処理が行われる（ステップ３２）。解凍は、たとえば自己解凍形式で自動的に行われるようにしても良い。なお、この解凍の際、認証２データを参照することによりデコードされるようにする。このように認証２データを参照しなければ解凍できないようにすることにより、圧縮ファイルの不正コピーを防止できる。

【００３８】圧縮ファイルの解凍により、クライアント側のシステムには、コンテンツ、認証３データ、および実行プログラムが利用可能な状態で保持される（ステップ３３）。なお、実行プログラムは、認証２データを参照しなければ起動できないようにすることができる。これにより、解凍後のコンテンツの不正利用を防止することができる。

【００３９】図４は、クライアント側におけるコンテンツの再生処理を説明するためのフローチャートである。まず、クライアントの端末は実行ファイルを起動する（ステップ４０）。この起動の際に前記認証２データを参照することができることは前記のとおりである。

【００４０】次に、コンテンツ内のヘッダを、有効期限を用いてデコードする（ステップ４１）。なお、このデコードに対応するエンコードは予めコンテンツデータに施されているとする。このように有効期限を用いてコンテンツデータをエンコードしておけば、コンテンツのみの不正なコピーを防止することができる。

【００４１】次に認証３データとして隠しファイルに格納された時間データを取得する（ステップ４２）。この取得した時間データを用いて、最終アクセス日時（最終利用日時）がシステムタイマ（ＣＰＵタイマ）の時間より前かを判断する（ステップ４３）。この判断がＮｏの時には、最終アクセス時間よりＣＰＵタイマの方が先にあるという正常使用の場合には本来生じない矛盾を生じる。このような場合、ＣＰＵタイマが不正に戻されたと判断して、時間データ（認証３データ）を破棄し（ステップ４４）、再生を中止する（ステップ３５）。このように認証３データ（時間データ）を破棄することにより、コンテンツデータのデコードが以後不可能になり、コンテンツの利用ができなくなる。

【００４２】一方、ステップ４３の判断がｙｅｓの場合、さらにＣＰＵタイマの時間が有効期限より前か（有効期限内か）を判断する（ステップ４６）。この判断がＮｏのとき、前記ステップ４３でも判断がＮｏの場合と同様に認証３データを破棄したうえで再生を中止する。有効期限を経過したコンテンツの利用を制限したものである。

【００４３】ステップ３６の判断がＹｅｓの時、コンテンツを再生する（ステップ３７）。前記ステップ３３および３６の判断を共にパスした場合のみ、有効期限内の正当使用と判断する。

【００４４】コンテンツの再生後、認証データ３の最終アクセス日時（最終利用日時）を更新する（ステップ３８）。更新された最終利用日時は、次回のコンテンツ利用の際に参照される。その後再生処理を終了する（ステップ３９）。なお、コンテンツがダウンロードされた際に、最終利用日時としてダウンロード日時を記録することができる。

【００４５】図５は、前記処理の流れを時系列に示した説明図である。ダウンロード時にダウンロード日時を最終利用日時としてデータファイル（認証３データ）に記録する。これを最終アクセス１とする。次に、時刻ｔ１で再生を開始するときに図４の処理を行えば、再生開始時（現在時刻）は最終アクセス日時よりあとであり、かつ有効期限内であるので、正常に再生が可能である。時刻ｔ２で再生が終了すれば、その時刻が最終アクセス２の最終利用日時として記録される。

【００４６】次に、時刻ｔ３で再生される場合、時刻ｔ１の場合と同様に再生が可能である。なお、再生途中で有効期限を経過しても、再生は最後まで行われる。

【００４７】有効期限経過後の時刻ｔ５で再生しようとした場合、現在時刻が有効期限（利用終了日時）を経過しているので、再生は不可能である。このとき、ユーザが不正に使用しようとしてシステムタイマ（ＣＰＵタイマ）をｔ７まで戻したとする。この場合、前記ステップ４６の判断はパスするが、前記ステップ４３の判断をパスしない。すなわち、前回の再生において、最終利用日時としてｔ４が最終アクセス３に記録されており、時刻ｔ７が時刻ｔ４より前になるという本来生じない矛盾を生じているためである。本実施の形態では、このような不正な利用を検出してこれを防止することが可能になる。

【００４８】なお、たとえば図５において、２度目の再

生操作（ｔ３～ｔ４）を行わず、本来再生不可能な３度目の再生操作（ｔ５～ｔ６）におけるタイマの不正操作（現在時刻を戻す操作）を時刻ｔ２と有効期限の間への変更として行った場合には、再生が可能であると共に最終利用日時が不正に繰り上がる。このような不正操作が繰り返されれば、実質的な有効期限の延長が可能になる恐れがある。このような場合、以下のような対策を施すことができる。

【００４９】すなわち、実行プログラム９と協働して作動しているたとえばＤＬＬ（dynamic link library）のような独立プログラムにシステムタイマとは別個のカウンタ手段を設ける。このような独立プログラムはシステムが稼動している間あるいは特定のＯＳが稼動している間は停止することがないので、コンピュータ（あるいはＯＳ）が稼動する限り有効期限を消費するように機能させることができる。つまり独立プログラムによるカウンタは常にシステム立ち上げ（あるいはＯＳ稼動開始）のときにシステムタイマによる現在時刻のアップデートを行う。実行プログラム９の実行開始時にシステムタイマの不正な時刻戻しが行われたかを判断し（不正なタイマ操作が行われたなら独立プログラムの時刻の方がシステムタイマより進むはずである）システムタイマを参照して不正操作分の期間を記録する。実行プログラム９の実行に際して、前記した最終アクセス日時と有効期限（あるいはＣＰＵタイマ（システムタイマ）の取得値）に前記期間の補正を加える。このような補正を加えた後の時刻データを用いて前記処理を実行できる。なお、最終アクセス日時と有効期限に補正を加える場合は前記期間を元の日時から減ずる補正、ＣＰＵタイマの取得値に補正を加える場合は取得値に前記期間を加える補正を行う。これにより、正当な有効期限の判断が行える。なお、最終アクセス日時と有効期限に補正を加えた場合には補正後の最終アクセス日時および有効期限を記録し、ＣＰＵタイマの取得値に補正を加えた場合は前記期間を記録し、以後の実行プログラムの処理の際に参照する。また、独立プログラムは実行プログラム９が最初に実行されるときにインストールされ、以後そのシステムが稼動する時には常時稼動するように機能させることは勿論である。

【００５０】以上、本発明者によってなされた発明を発明の実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更することが可能である。

【００５１】たとえば、前記実施の形態では、認証１，２の各データおよび認証３の時刻データ（利用開始日時）を用いて各ファイルあるいはプログラムのコピー防止の手段を説明した。しかし、コピー防止は前記方法に限られず、その他各種の手法を用いることができる。たとえば電子透かしの技術等である。

【００５２】また、前記実施の形態では、認証データの記録方法として、別ファイル（隠しファイル）を用いて格納する方法を説明したが、これに限られない。たとえばコンテンツ自体に有効期限を埋め込む方法、あるいは、実行プログラム自体に有効期限を埋め込む方法を適用してもよい。

【００５３】また、前記実施の形態において、再生途中でのシステムタイマの戻し操作を禁止するようにしても良い。

【００５４】また、前記実施の形態では、クライアント側のシステムとして、コンピュータシステム２、携帯電話３、ＰＤＡ４を例示したが、これに限られない。たとえばインターネット１に接続可能なビデオ再生機等を例示できる。この場合、ビデオデータのヘッダ領域に時間情報その他の認証データを埋め込み、この認証データを利用して前記した各種の認証を行うことができる。

【００５５】また、前記した実施の形態では、コンテンツの配信要求に応答してサーバ５がコンテンツと必要な認証データを同時に送付する例を説明したが、コンテンツと認証データの配信時期を異ならせても良い。たとえば、クライアントからの要求に応じて、まず認証データ（有効期限情報とコンテンツを再生・実行するに必要なデータ）を送付し、クライアントがコンテンツの再生・実行を望む時にその都度コンテンツを配信するオンデマンド配信を行っても良い。この場合、オンデマンド配信されたコンテンツは先に入手した認証データを用いて前記実施の形態に記載したような再生・実行処理（認証処理）を行い、コンテンツの利用が可能になる。また、事前に入手する認証データについては、所定範囲のコンテンツについて包括的に認証が与えられても良い。つまり認証データとコンテンツとは一対一に対応する必要は無く、複数のコンテンツあるいは将来提供される予定のコンテンツに対して１つの認証が与えられても構わない。

【００５６】

【発明の効果】本願で開示される発明のうち、代表的なものによって得られる効果は、以下の通りである。すなわち、コンテンツ利用に有効期限を設けた場合に、ユーザの不正なコンテンツ利用を防止することができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態であるコンテンツ配信方法を実現するシステムの一例を示した概念図である。

【図２】端末側のシステム（クライアント）とサーバ５のシステムを示したブロック図である。

【図３】本発明の一実施の形態であるコンテンツ配信方法の一例を示したフローチャートである。

【図４】クライアント側におけるコンテンツの再生処理を説明するためのフローチャートである。

【図５】前記処理の流れを時系列に示した説明図である。

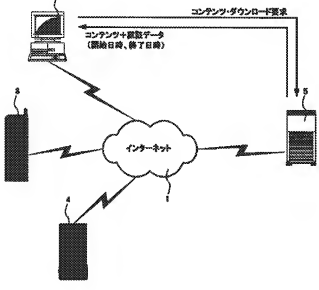
【符号の説明】

１…インターネット、２…コンピュータシステム、３…

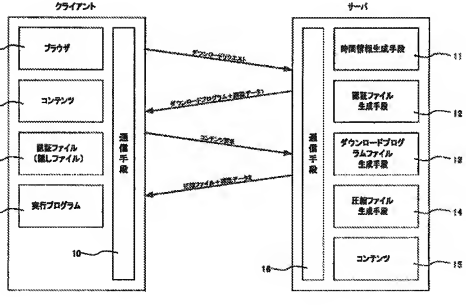
15　　16

携帯電話、４…携帯情報端末、５…サーバ、６…ブラウザ、７…コンテンツ、８…認証ファイル、９…実行プログラム、１０…通信手段、１１…時間情報生成手段、１２…認証ファイル生成手段、１３…ダウンロードプログ＊ラムファイル生成手段、１４…圧縮ファイル生成手段、１５…コンテンツ、１６…通信手段、ｔ１～ｔ７…時刻。

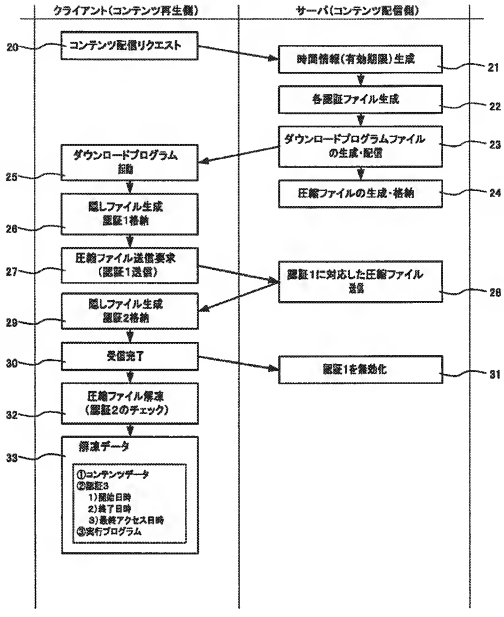
【図１】



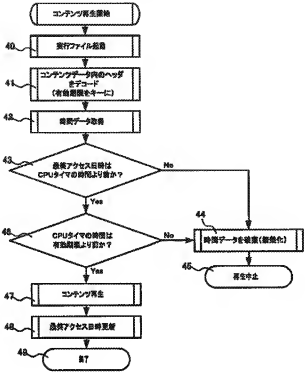
【図２】



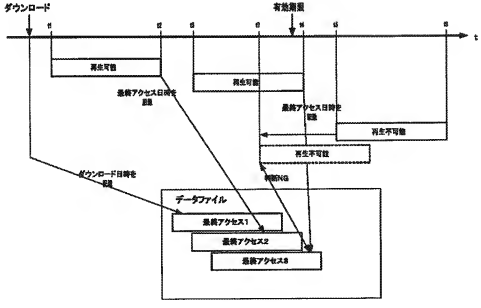
【図３】


クライアント(コンテンツ再生側)
サーバ(コンテンツ配信側)
20
コンテンツ配信リクエスト
時間情報(有効期限)生成
21
各認証ファイル生成
22
ダウンロードプログラムファイル
の生成・配信
23
ダウンロードプログラム
起動
25
圧縮ファイルの生成・格納
24
隠しファイル生成
認証1格納
26
圧縮ファイル送信要求
(認証1送信)
27
認証1に対応した圧縮ファイル
送信
28
隠しファイル生成
認証2格納
29
受信完了
30
認証1を無効化
31
圧縮ファイル解凍
(認証2のチェック)
32
解凍データ
33
①コンテンツデータ
②認証3
1)開始日時
2)終了日時
3)最終アクセス日時
③実行プログラム

【図４】



【図５】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード（参考）
G06F 17/60	512	G06F 17/60	512	
H04L 9/32		H04N 7/173	620D	
H04N 7/167		H04L 9/00	675D	

7/173　　６２０　　H０４N　7/167　　Z

(72)発明者　森　昌也
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　大和事業所内
(72)発明者　岡本　順子
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　大和事業所内

Ｆターム(参考)　5B017 AA07 BB10 CA15 CA16
5B085 AC05 AE23 BG07
5C064 BA07 BB10 BC17 BC18 BC22
BC23 BC25 BD02 BD08 BD09
CA14 CB01 CC04
5J104 AA07 AA14 KA02 PA14